20-1653(L)

20-3945(CON)

In the

United States Court of Appeals

For the Second Circuit

In re: In the Matter of the Search of Information Associated with Specified E-Mail Accounts

Microsoft Corporation,
Appellant

v.

United States of America,
Appellee

On Appeal from the United States District Court
for the Eastern District of New York (Brooklyn)

Brief for *Amicus Curiae* BSA | The Software Alliance In Support of Appellant

Yaira Dubin
O'Melveny & Myers LLP
7 Times Square
New York, NY 10036
(212) 326-2000
ydubin@omm.com

Michael R. Dreeben
Ephraim McDowell
O'Melveny & Myers LLP
1625 Eye Street, N.W.
Washington, DC 20006
(202) 383-5300
mdreeben@omm.com
emcdowell@omm.com

Counsel for BSA | The Software Alliance

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1(a) and Second Circuit Rule 26.1, *amicus curiae* BSA | The Software Alliance states that it is not a publicly held corporation and has no parent company. No publicly held company owns 10% or more of its stock.

Dated: December 21, 2020

By: /s/ Michael R. Dreeben
Michael R. Dreeben

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

Other Authorities

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Rules

INTEREST OF *AMICUS CURIAE*[1]

Amicus BSA | The Software Alliance is the leading association representing the software industry before governments and in the international marketplace. BSA promotes policies that foster innovation, growth, customer trust, and a competitive marketplace for commercial software and related technologies. Many BSA members either design or operate significant cloud computing networks. BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC Software—Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce.com, ServiceNow, Siemens Industry Software, Inc., SiteCore, Slack, Splunk, Inc., Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

BSA submits this *amicus* brief because it has a significant interest in ensuring the sustained success of the cloud services industry—a vital segment of the American economy. That industry depends on the trust that customers place in cloud service providers to protect their data. To maintain that trust, when the Government demands a customer's data, a cloud service

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), counsel for BSA states that no counsel for a party authored this brief in whole or in part, and no person—other than BSA, its members, or its counsel—made a monetary contribution intended to fund the preparation or submission of this brief. All parties to this appeal have consented to the filing of this brief.

provider must be allowed to notify the customer in all but the most unusual circumstances. The First Amendment protects the provider's right to do so: a restriction on the provider's speech is unconstitutional unless it is narrowly tailored to achieve a compelling interest. The Government has not met that high threshold in this case. Upholding nondisclosure orders that fail to meet First Amendment requirements, like the one at issue here, threatens to undermine the customer trust that is essential to the cloud services industry.

INTRODUCTION

This case raises a question of fundamental importance for BSA, its members, and the cloud services industry: when does the Constitution protect a cloud service provider's right to notify its customer that the Government has demanded that customer's data in a criminal investigation? The Stored Communications Act (SCA) permits the Government to seek a nondisclosure order against a cloud service provider when certain conditions are met. *See* 18 U.S.C. § 2705(b). But under the First Amendment, those orders should be the exception, not the rule. The First Amendment imposes stringent requirements to ensure that speech—especially speech about the Government's activities—is not impermissibly restrained.

BSA recognizes that, in some cases, nondisclosure orders may be justified to protect compelling governmental interests in the integrity of

criminal investigations. But nondisclosure orders constitute content-based prior restraints on speech. That form of speech restriction requires the most rigorous form of review: strict scrutiny. Under that standard, a speech restriction must fail unless the Government can show that it is narrowly tailored to achieve a compelling interest. When the Government has less-restrictive alternatives that will achieve its interests, broader restrictions are impermissible. And courts must remain vigilant to ensure that the Government meets its heavy burden.

Exacting enforcement of these First Amendment principles is essential to the cloud services industry. That industry depends on customer trust that cloud service providers will safeguard customers' most sensitive data. Unless cloud service providers can regularly inform customers when the Government has demanded and seized their data, customer trust may erode. That erosion of customer trust has the potential to undermine the growth of the cloud computing environment and lead customers to resort to less-efficient, less-secure data-storage arrangements. And that, in turn, will harm the American economy, which increasingly relies on cloud computing. Because the district court misapplied the stringent First Amendment standards that govern content-based prior restraints on speech, this Court should reverse.

ARGUMENT

I. Cloud Computing Is Critical To The American Economy

"Cloud computing uses remote servers and networks for data storage which may be accessed using web-enabled devices, such as computers, tablets, or smart phones." *Smith v. Barnesandnoble.com, LLC*, 839 F.3d 163, 166 (2d Cir. 2016). A cloud-based technology user can remotely store, access, and process data through the internet, rather than on the user's desktop computer or local server. Cloud service providers operate the hardware and software that allow for these data storage and processing activities.

Cloud computing services have become a fixture of American life and business: both "[i]ndividuals and enterprises are increasingly moving their data to the 'cloud.'" U.S. Dep't of Justice, *Seeking Enterprise Customer Data Held By Cloud Service Providers* (Dec. 2017) ("Recommended Practices"), JA-20. Cloud computing services—used every day by countless Americans at home and work—include raw computing resources (such as processing and storage capacity), development and deployment platforms (such as web servers and database-management systems), and software applications (such as customer-relationship management or business-analysis tools). Common uses of the cloud include e-mail and messaging services; document

management; database management; collaboration tools; human-resources services; data analytics; research tools; and artificial-intelligence services.

Enterprises, such as corporations, government agencies, and universities, have become increasingly dependent on cloud computing services for their most essential functions. For example, many American businesses now store their most sensitive information on the cloud—from employee emails, to customer information, to business plans, to trade secrets. But the cloud is more than an electronic storage locker. Cloud-based technologies also underpin a range of services used every day by businesses in every economic sector. Those cloud-based services include communications tools like e-mail and messaging services; workplace-collaboration tools like videoconferencing (made all the more important because of COVID-19); and software to help companies manage their customer interactions or administer human-resources functions like processing payroll or employee benefits. This increased use of cloud computing services helps businesses grow and thrive for several reasons.

First, cloud computing provides an efficient mechanism for storing and processing data. Before the advent of cloud computing, companies "kep[t] and process[ed] large amounts of data in-house" on local computers and servers. Michael W. Price, *Rethinking Privacy: Fourth Amendment*

"Papers" and the Third-Party Doctrine, 8 J. Nat'l Security L. & Pol'y 247, 295 (2016). With cloud computing, by contrast, companies can outsource these functions to cloud service providers that distribute data storage and processing "among a global network of millions of computers." *Id.*[2] Similarly, companies no longer need to "purchase enough capacity to meet maximum demand," but rather can "purchase only the computing services they actually use." Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 328-29 (2013). In short, "commercial cloud computing" leads to "cost savings for a business over internally managing data." Amy L. Stein, *Artificial Intelligence and Climate Change*, 37 Yale J. on Reg. 890, 932 (2020).[3]

Second, cloud computing provides enhanced security and reliability. A large-scale cloud service provider has more resources to combat hacking and intrusions than an individual company fending for itself. Cloud service

---

[2] *See also* Michael L. Rustad & Elif Kavusturan, *A Commercial Law for Software Contracting*, 76 Washington & Lee L. Rev. 775, 870 (2019) (cloud computing "enable[s] many customers to share a large pool of storage and common computing resources").

[3] *See also* Zach Lanich, *The Benefits of Moving to the Cloud*, Forbes (May 19, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/05/19/the-benefits-of-moving-to-the-cloud/?sh=7754399e4733 ("Cloud services allow you to pay for the resources usage you need while taking advantage of scale and reliability, two things that most companies can't afford internally.").

providers share the cost of security "across a large virtualized cloud of computers" and cultivate security "expertise" through vast and varied experience. Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761, 1821-22 (2011). "Very experienced staff maintain [cloud service] infrastructures, processes are tight[,] and there are many eyes on these systems at all times." Lanich, *supra* note 3. An individual company simply cannot replicate this sort of sophisticated, stress-tested security apparatus. This is why most security professionals now agree that storing data on the cloud is as safe or safer than storing it on a company's premises.[4]

Third, cloud services provide businesses and their employees greater flexibility in accessing and using their data. These services allow customers "to instantly access their data from a web-connected computer anywhere in the world." *Hately v. Watts*, 917 F.3d 770, 792 (4th Cir. 2019) (quoting Cristopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. Telecomm. & High Tech. L. 359, 361 (2010)). For customers, "cloud services generally eliminate the geographic location of hardware … as a relevant aspect of computing." Andrews & Newman, 73 Md. L. Rev. at 326. "So long as a network connection

[4] *See* Anthony Spadafora, *Businesses Are Finally Starting To Trust the Cloud*, TechRadar (Sept. 4, 2019), https://www.techradar.com/news/businesses-are-finally-starting-to-trust-the-cloud.

exists, the physical location of end users, servers, and service providers—and their proximity to one another—is almost entirely irrelevant." *Id.* The ability to access data remotely from nearly anywhere in the world has become indispensable during the COVID-19 pandemic. As a result, "companies across the economy [have] rel[ied] more heavily on remote workplace tools and cloud-based technologies that help employees remain productive while working outside of their physical offices."[5]

The foregoing benefits of cloud computing are reflected in the industry's significant contributions to economic growth. By 2025, the total potential economic impact of cloud technology could be between $1.7 and $6.2 trillion, including a $500-$700 billion impact through information-technology productivity improvements for businesses.[6] And during the COVID-19 pandemic, cloud technology has proved to be "an enabler of

[5] Testimony of Victoria A. Espinel, President and CEO BSA | The Software Alliance, Senate Committee on Commerce, Science, and Transportation, at 2 (Dec. 9, 2020), bsa.org/files/policy-filings/12092020bsaprivacy shieldtestimony.pdf.

[6] James Mankiya et al., *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy*, McKinsey & Co., at 63 (May 2013), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.pdf.

increasingly critical e-commerce, remote sales, and flexible cost structures."[7] In sum, cloud computing ranks as "one of the most significant technical advances for global business in this decade—as important as PCs were to the 1970s." Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 Am. Bus. L.J. 413, 418 (2013) (internal quotation marks omitted).

II. The Cloud Services Industry Depends On Customer Trust, Which Would Be Undermined If The Government Could Routinely Obtain Customer Data From Cloud Service Providers Without Customer Notification

A. As explained above, many enterprises have moved their most essential and sensitive data from their own servers to the cloud. In making that move, these enterprises have not relinquished their rights and interests in their data. To the contrary, data stored with a cloud service provider *is* the "customer's[] data"—*not* the cloud service provider's. BSA | The Software Alliance, *BSA Global Best Practices For Law Enforcement Access To Digital*

[7] McKinsey & Company, *Making the Cloud Pay: How Industrial Companies Can Accelerate Impact From the Cloud* (Oct. 1, 2020), https://www.mckinsey.com/industries/advanced-electronics/our-insights/making-the-cloud-pay-how-industrial-companies-can-accelerate-impact-from-the-cloud.

Evidence, at 4.[8] Customers (quite properly) view their cloud storage environments as an extension of their own infrastructure, and they correspondingly demand certainty and transparency about how their data is processed and accessed.

This view of data stored in the cloud accords with the Supreme Court's recent recognition that constitutionally protected interests in digital data do not vanish simply because that data is stored with a third party. In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court held that a person had a protected Fourth Amendment expectation of privacy in "cell phone location information" stored with a wireless-telephone carrier in large measure because that information provides "a detailed and comprehensive record of the person's movements." *Id.* at 2216-17. And in *Riley v. California*, 573 U.S. 373 (2014), the Court similarly emphasized the important privacy interests implicated by the immense "storage capacity of cell phones"—which

[8] *See* https://www.bsa.org/files/policy-filings/09232019leaglobalbestpractices.pdf; *see also* BSA | The Software Alliance, *Data Privacy*, https://www.bsa.org/policy-issues/privacy ("BSA members are committed to protecting the privacy and security of consumers' data. BSA promotes a user-centric approach to privacy that provides consumers with control over their personal data while ensuring industry can continue delivering value to consumers by providing innovative products and services.").

includes "files stored in the cloud"—in limiting cell-phone searches as a routine procedure incident to a person's arrest. *Id.* at 394, 397.[9]

These considerations carry even greater force in the context of enterprise cloud-based storage: Because of the "detailed and comprehensive" nature of the information that enterprises store with cloud service providers, these enterprises have substantial and enduring interests in the privacy and control of that information. *Carpenter*, 138 S. Ct. at 2217. The enterprise's privacy and proprietary interests are not at all diminished by its decision to store its information in the cloud; the improvements that cloud-based technology provides do not erase the interests that the enterprise would unquestionably have in its data if that data were stored on-site.

In light of these weighty interests, enterprises trust and expect cloud service providers to safeguard their data. *See* Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust With United*

[9] *See also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) ("In the 'cloud,' a user's data, including the same kind of highly sensitive data one would have in 'papers' at home, is held on remote servers rather than on the device itself."); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that an email "subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial" internet service provider (quotation marks omitted)).

States Companies, 16 J. of Tech. Law & Pol'y 229, 236 (2011) (noting the "great amount of trust and assurance" a company must place in "a cloud provider").[10] And providers, in turn, "are obliged to protect the trust and confidence of their customers, including in relation to customer privacy and security." BSA | The Software Alliance, *Global Best Practices for Law Enforcement Access to Digital Evidence*, at 4.[11] If enterprises cannot not trust cloud service providers, those enterprises will seek alternatives, *cf.* Barry Friedman & Elizabeth G. Janszky, *Policing's Information Problem*, 99 Tex. L. Rev. 1, 21 (2020) (noting that revelation of the National Security Agency's bulk-data collection program led to "a flight from American cloud computing companies")[12]—including potentially reverting back to the

[10] *See also* Siani Pearson, *Privacy, Security and Trust in Cloud Computing*, HP Laboratories, at 43 (2012) ("Companies who change from carrying out their computing in-house to using the public cloud are not so much concerned any more about the health of servers, but instead the confidentiality and security of their data.").

[11] *See also* BSA | The Software Alliance, *Global Privacy Best Practices*, at 1, https://www.bsa.org/files/policy-filings/2018_BSA_Global_Privacy_Best_Practices.pdf ("[T]he protection of personal data is an important priority for BSA members, and we recognize that it is a key part of building customer trust.").

[12] *See also* Ben Rossi, *Are Companies Right To Finally Trust Public Cloud?*, Information Age (June 14, 2016), https://www.information-age.com/are-companies-right-finally-trust-public-cloud-123461605/ (noting that while the "cloud has grown enormously as an enterprise solution," the only thing that has sometimes "held it back [is] a lack of trust").

inefficient and less-secure prior regime of storing data on local servers. If that were to occur, the economic benefits, convenience, and efficiency that cloud computing provides to American companies would no longer be realized.[13] And America's leadership in digital innovation would be threatened.

B. When the Government is conducting a criminal investigation that requires it to collect data from cloud service providers' enterprise customers, the ordinary, appropriate, and effective way to do that is through a request or legal process to the relevant enterprise itself. That is what the Government routinely and necessarily did before the advent of cloud computing. And that established method is essential to protecting the subject enterprise's core procedural rights and the integrity of its information. The Government should not be permitted to exploit new technologies like the cloud as a way to end-run these vital rights and interests. *Cf. Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("technology" cannot "erode the privacy guaranteed by the Fourth Amendment").

Most fundamentally, legal process directed to the enterprise customer gives it notice of the investigation, allowing it to retain counsel. The

[13] *See* King & Raja, *supra*, at 418 ("To reach its potential, the [cloud computing] industry must build consumers' trust that their sensitive data, which will be stored and processed in the cloud, will be private and secure.").

enterprise's counsel can then engage with the Government on the scope of the inquiry, the applicability of any privileges, and ways to meet the Government's legitimate needs without jeopardizing the integrity or confidentiality of the enterprise's information. Beyond that, approaching the enterprise directly facilitates its ability to segregate relevant from irrelevant information. The enterprise customer itself—with deep knowledge of its own data—is best equipped to assert these protections. *See, e.g.*, *Upjohn Co. v. United States*, 449 U.S. 383 (1981) (corporation asserting numerous privileges in white-collar investigation). Cloud service providers hosting the data are not—indeed, such providers may lack visibility into the contents of their customer's data because of data-encryption practices and privacy agreements. *See infra* at 17.

Directing legal process to the customer can also enable it to secure pre-compliance judicial review where appropriate. *See City of Los Angeles v. Patel*, 576 U.S. 409, 420 (2015). This is particularly important where—as is often the case—legal process initially seeks an overly broad set of records. Courts have recognized "the reality that over-seizing is an inherent part of the electronic search process" and that "this reality call[s] for judicial officers to exercise greater vigilance in protecting against the danger that the process of identifying seizable electronic evidence could become a vehicle for the

government to gain access to a larger pool of data that it has no probable cause to collect." *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (internal quotation marks omitted).

And once the Government has acquired electronic information, that information does not automatically vanish. This Court has observed that massive potential intrusions on "privacy" are "implicated when a hard drive or forensic mirror is retained, even pursuant to a warrant," potentially permitting its search months or even years later. *United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2018) (en banc). That is not only because of the quantity of data stored on computers, but because of "the significance of the data kept by many individuals on their computers." *Id.* at 218 (noting that individuals store "[t]ax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, banking and shopping information … interspersed among the evidentiary material that justifies the search or seizure"); *see also United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (recognizing that "[a] general search of electronic data is an especially potent threat to privacy"). Those dangers are magnified with the vast troves of data an enterprise customer may keep in cloud storage. Courts are well positioned to limit the intrusiveness of electronic searches—but only if the subject of the search can ask them to do so. In the

SCA context, an enterprise customer needs notice of the warrant in order to assess and potentially assert its legally available protections.

The Government itself has recognized that its primary investigative avenue should be through the relevant enterprise. Department of Justice guidelines correctly observe that before cloud computing, "prosecutors had to approach a company or similar enterprise directly for electronic data stored on servers located on an enterprise's premises." DOJ Recommended Practices, JA-20. And those guidelines make clear that the Department should adhere to the same general practice today by "seek[ing] data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation." *Id.* "This approach," the guidelines emphasize, "gives [enterprise] counsel the opportunity to interpose privilege and other objections to disclosure for appropriate resolution, and parallels the approach that would be employed if the enterprise maintained data on its own servers." JA-21.

In fact, this enterprise-focused approach will frequently benefit the Government's own interests in conducting an efficient investigation. *See* JA-20 (noting "the lengthier time often required to obtain the information useful to an investigation by seeking enterprise data from a cloud provider"). Given that enterprises will have intimate familiarity with the nature and

organization of their own data, they will be better situated to readily gather relevant data than cloud service providers. That is particularly true because enterprises sometimes "encrypt data on [their] own systems before transmitting [it] to their cloud provider." JA-21. They also may negotiate contractual provisions precluding cloud service providers from accessing data except in limited circumstances. Accordingly, the Government can—and regularly does—directly ask enterprises to produce information they store in the cloud.

C. Still, cases may arise where the Government has a compelling reason to seek data from the cloud service provider, as opposed to the enterprise customer. BSA fully appreciates that cloud service providers sometimes "play an important role in responding to law enforcement efforts to request digital evidence in criminal investigations." BSA | The Software Alliance, *BSA Global Best Practices for Law Enforcement Access to Digital Evidence*, at 4. And, upon receipt of appropriate legal orders, BSA members aim "to help law enforcement process the huge amounts of data [it] must … manage in today's investigations." BSA | The Software Alliance, *More Data Is Available To Law Enforcement Than Ever Before*.[14]

[14] *See* https://www.bsa.org/files/policy-filings/BSA_Encrypt_AvailabilityData-web.pdf.

But the cases in which the Government approaches a cloud service provider for an enterprise customer's data should be exceedingly rare. As Department of Justice guidelines explain, the Government should "seek[] disclosure directly from the cloud provider" when that is "the *only* practical option." DOJ Recommended Practices, JA-21-22 (emphasis added). For example, this could be true when "an enterprise is essentially devoted to criminal activity," as with "a small medical practice suspected of engaging in massive Medicare fraud," JA-21, or even with a larger company whose executives and employees are suspected of pervasively engaging in criminal conduct, *see, e.g.*, *Skilling v. United States*, 561 U.S. 358, 368 (2010) (describing "an elaborate conspiracy to prop up Enron's short-run stock prices" involving "dozens of Enron employees").

In the rare cases in which the Government must seek an enterprise customer's information from a cloud service provider, the First Amendment requires that the provider be permitted to notify the affected customer—unless the Government can show that a nondisclosure order is essential to protecting its investigation, and no other more nuanced or tailored remedy would protect its legitimate interests.[15] Notifying enterprises of law-

[15] Recent proposed EU legislation on this subject suggests a similar approach: "The service provider shall inform the person whose data is being

enforcement demands for their information is critical to preserving the customer trust and confidence underlying cloud service providers' business models. As BSA has explained, to promote that trust-based relationship, providers "should notify their customers of government requests for the customers' information unless prohibited from doing so." BSA | The Software Alliance, *Principles: Additional Safeguards for SCC Transfers* (Oct. 2020)[16]; *see* BSA | The Software Alliance, *BSA Global Best Practices for Law Enforcement Access to Digital Evidence*, at 4 (advocating customer notification to promote "the trust and confidence of [providers'] customers"); JA-62 (district court discussing Microsoft's commitment to notifying customers of law-enforcement data requests).

---

sought without undue delay. … [T]he issuing authority, taking into due account the impact of the measure on the fundamental rights of the person whose data is sought, may request the service provider to refrain from informing the person whose data is being sought, based on a judicial order. Such an order shall be duly justified, specify the duration of the obligation of confidentiality and shall be subject to periodic review." Draft European Parliament Legislative Resolution, On the Proposal For a Regulation of the European Parliament and of the Council on European Production and Preservation Orders For Electronic Evidence in Criminal Matters, Art. 11, https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html.

[16] *See* https://www.bsa.org/files/policy-filings/10222020bsascctransfers.pdf.

If a cloud service provider is barred from speaking with its enterprise customer, the provider's trust-based relationship with its customer will be undermined. *See* Khaled M. Khan & Qutaibah Malluhi, *Establishing Trust in Cloud Computing*, IT Professional, at 25 (Sept./Oct. 2010) (customer "trust" depends on "cloud providers … offer[ing] better transparency").[17] In turn, the customer may be deterred from fully utilizing cloud computing services. Aggregated across the cloud services industry, the effects of precluding cloud service providers from notifying their customers of law-enforcement data requests could inflict substantial harm on this vibrant and vital sector of the American economy.

III. This Court Should Enforce The First Amendment's Rigorous Standards And Hold The Nondisclosure Order Here Unconstitutional

Proper application of the First Amendment will stave off these harmful consequences and protect cloud service providers' trust-based relationships with their customers, without jeopardizing criminal investigations. Nondisclosure orders against cloud service providers are content-based prior restraints on speech, subject to strict scrutiny. The Government can rarely meet its burden under that stringent standard, and it has not done so

[17] *See* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.6574&rep=rep1&type=pdf.

here. Three features of this case render the nondisclosure order unconstitutional: (1) the Government's failure to adequately explain why it cannot accommodate Microsoft's reasonable, less-restrictive alternative of notifying one trustworthy individual at the subject enterprise; (2) the Government's undue reliance on *ex parte* filings, which impedes the traditional adversarial process; and (3) the prolonged timeframe in which the Government has suppressed Microsoft's speech.

A. The Nondisclosure Order Here Implicates Core First Amendment Protections Against Content-Based Prior Speech Restraints

A cloud service provider has a First Amendment right to notify its customer when the Government demands or seizes that customer's data. The Government can overcome that right only by carrying its burden of proof under the most rigorous of legal standards.

Two bedrock First Amendment principles establish the heavy burden the Government must shoulder to suppress cloud service providers' speech. First is the rule against prior restraints of speech. A prior restraint "forbid[s] certain communications … in advance of the time that such communications are to occur." *Alexander v. United States*, 509 U.S. 544, 550 (1993). "[P]rior restraints on speech … are the most serious and the least tolerable infringement on First Amendment rights." *Neb. Press Ass'n v. Stuart*, 427

U.S. 539, 559 (1976). That is because a "[p]rior restraint upon speech suppresses the precise freedom which the First Amendment sought to protect against abridgement." *Carroll v. President & Comm'rs of Princess Anne*, 393 U.S. 175, 181 (1968); *see id.* at 181 n.5 ("The elimination of prior restraints was a leading purpose in the adoption of the First Amendment." (internal quotation marks omitted)). Thus, "prior restraints of expression come[] to this Court bearing a heavy presumption against [their] constitutional validity." *Id.* at 181 (internal quotation marks omitted). The nondisclosure order here qualifies as a prior restraint because it precludes Microsoft from speaking to its customer *ex ante*, rather than penalizing its speech *ex post*.

The second First Amendment principle at issue is the suspect character of content-based speech restrictions. "Above all else, the First Amendment means that government generally has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *Barr v. Am. Ass'n of Pol. Consultants, Inc.*, 140 S. Ct. 2335, 2346 (2020) (plurality) (internal quotation marks omitted). "Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). The nondisclosure order here targets Microsoft's speech based on its content—

namely, it prevents Microsoft from conveying a "particular … message" informing its customer that the Government has seized that customer's data. *Id.* That type of message—one concerning "the exercise of the State's power"—"lies at the very center of the First Amendment." *Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1034 (1991); *see John Doe, Inc. v. Mukasey*, 549 F.3d 861, 878 (2d Cir. 2008) (information "relevant to intended criticism of a governmental activity" is core First Amendment speech).[18] The ability to convey that message is critical so that cloud service providers like Microsoft can maintain the trust on which their customer-provider relationships are built.

Because the nondisclosure order is a content-based prior restraint on speech, the Government bears the burden of showing that the order satisfies strict scrutiny. *See Barr*, 140 S. Ct. at 2347; *Carroll*, 393 U.S. at 181. Strict scrutiny "requires the Government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Reed*, 576 U.S. at 171 (internal quotation marks omitted). "[I]t is the rare case in which [the Supreme Court] ha[s] held that a law survives strict scrutiny."

[18] *See also Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829, 838 (1978) ("a major purpose of [the First] Amendment was to protect the free discussion of governmental affairs"); *Mills v. Alabama*, 384 U.S. 214, 218 (1966) (same).

Burson v. Freeman, 504 U.S. 191, 211 (1992) (plurality). In recent years, the Supreme Court has regularly invalidated unjustified speech restrictions under that demanding standard.[19]

B. The Nondisclosure Order Here Fails Strict Scrutiny

In this case, the Government has deviated from DOJ guidelines in two respects: instead of approaching Microsoft's customer directly, it issued legal process only to Microsoft; and instead of allowing Microsoft to notify its customer of the SCA warrant, it sought a nondisclosure order. That nondisclosure order does not satisfy strict scrutiny, and the district court erred in holding otherwise.

BSA does not dispute that the Government has a compelling interest in maintaining the integrity of this particular criminal investigation. But upholding this prohibition on Microsoft's right to communicate with its customer violates the First Amendment and would produce a troubling precedent for the cloud services industry for three reasons. First, the Government has failed to show that Microsoft's reasonable, less-restrictive

[19] *See, e.g.*, *Barr*, 140 S. Ct. at 2347; *Reed*, 576 U.S. at 171-72. The Court has upheld speech restrictions under strict scrutiny only in extraordinary circumstances, such as where the relevant restriction "prohibit[ed] judges and judicial candidates from personally soliciting funds for their campaigns," which served to "assure [the] people [of a state] that judges will apply the law without fear or favor." *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 437 (2015).

alternatives to a blanket prohibition on its speech would be ineffective; second, the Government's *ex parte* filings excessively shrouded its justifications in secrecy, thus interfering with the proper adversary process; and third, the nondisclosure order's duration raises concerns about undue suppression of speech.

***1. Failure to Accommodate Reasonable Alternatives*:** "When a plausible, less restrictive alternative is offered to a content-based speech restriction, it is the Government's obligation to prove that the alternative will be ineffective to achieve its goals." *United States v. Playboy Entm't Grp.*, 529 U.S. 803, 816 (2000). This "burden on the Government to explain why a less restrictive [alternative] would not be as effective" is "an especially heavy" one here because of "[t]he breadth of th[e] content-based restriction of speech." *Reno v. ACLU*, 521 U.S. 844, 879 (1997).

Microsoft has offered a less-restrictive alternative to the Government's blanket nondisclosure order: notify one individual at the subject company of the Government's data demand—for instance, a company officer, director, or lawyer. *See* Microsoft Br. 22, 30. And at a minimum, Microsoft proposed to inform the designated individual only of the fact that Microsoft had received a warrant seeking information about the company, without disclosing the employee e-mail addresses targeted by the Government's warrant. *Id.* at 12,

23. These reasonable, middle-ground solutions would promote Microsoft's interest in maintaining customer trust, without jeopardizing the Government's investigation.

Yet the Government has rebuffed Microsoft's proposals—even though it has embraced similar proposals both in Department of Justice guidelines and other individual cases. DOJ guidelines recommend that prosecutors consider "whether any protective order can be narrowed to permit the provider to notify an appropriate official at the enterprise without posing a risk to the integrity of the investigation." DOJ Recommended Practices, JA-22-23. And in a different case involving Microsoft, the Government recently agreed "to notify an individual at the Enterprise Customer about the [data-production] orders, including by providing an individual at the Enterprise Customer with the account targeted." *Microsoft Corp.'s Appeal of Non-Disclosure Orders*, No. 1:20-mc-00349, ECF 1 (S.D.N.Y. Oct. 16, 2020). This type of narrow agreement is what Microsoft seeks here as well. The Government bears a heavy burden to show that an alternative that it has previously accepted is now somehow untenable here.

The Government cannot plausibly show that *no one* at the subject enterprise could be notified without jeopardizing the Government's investigation. Many large enterprises maintain robust compliance

departments staffed with attorneys and other professionals tasked with addressing internal misconduct. *See, e.g.*, 15 U.S.C. § 7262 (requiring publicly-traded corporations to file annual reports describing internal-control programs). And at a minimum, an enterprise's general counsel, or another attorney in its legal department, should be a trustworthy recipient of sensitive information. *See* DOJ Recommended Practices, JA-21 (noting that an enterprise's "general counsel or legal representative" are often "appropriate contact[s]" for law enforcement); Adam Rahman, *Cooperation and Its Discontents: The Constitutional and Policy Implications of the DOJ's War on Corporate Crime*, 14 Geo. J.L. & Pub. Pol'y 323, 338 (2016) ("[p]rosecutors are often in day-to-day contact with corporate counsel while an internal investigation is underway"). Where, as here, the Government's investigation focuses on "just two employees" at "a major international corporation," it is unrealistic to say that *nobody* at that corporation could safely receive notification. Microsoft Br. 9; *see* JA-24.

To justify its stringent ban, the Government bears the burden to provide specific facts showing that Microsoft's proposed "alternative will be ineffective," *Playboy Entm't Grp.*, 529 U.S. at 816—*i.e.*, that it would seriously risk the investigation's integrity. Absent such a showing, the nondisclosure order's curtailment of Microsoft's right to speak to its

customer—the pillar of Microsoft's customer-provider relationship—is unconstitutional. Here, the district court found only "*possible* involvement of additional employees" and "*possible* corporate criminal liability," JA-95 (emphasis added), which does not suggest that notifying a single individual at the company—again, an alternative that DOJ guidelines themselves expressly recommend—would jeopardize the Government's investigation. And the district court's rejection of Microsoft's proposal because it "was not *as effective* as the nondisclosure order in achieving the Government's purpose," JA-93 (emphasis added), fundamentally misunderstands the strict scrutiny inquiry. A sweeping speech restriction will *always* be most effective in serving the Government's secrecy interest—but the First Amendment permits content-based restrictions only when the Government shows that the speaker's proposed alternative would be "*ineffective*." *Playboy Entm't Grp.*, 529 U.S. at 816 (emphasis added); *see Ashcroft v. ACLU*, 542 U.S. 656, 668 (2004) (less-restrictive alternative need not be "perfect solution").

The district court also asserted that Microsoft's proposed alternative would shift "the burden on speech … to others—employees at the targeted company—who presumably owe a duty of loyalty to the company." JA-93 n.7. But neither the district court nor the Government cited any authority suggesting that every company officer or lawyer would violate a fiduciary

duty by maintaining the secrecy of confidential information about a Government investigation. In fact, compliance officers and in-house counsel regularly handle sensitive information about internal corporate malfeasance. *See* 15 U.S.C. § 78j-1(m)(4) (requiring publicly-traded corporations to establish procedures to handle internal complaints and whistleblowing about fraudulent conduct); Erin M. Carter, *Pragmatic Selective Waiver: Re-Aligning Corporate Executives' Personal Interests With Those of the Corporation Amidst Government Investigations*, 62 Vand. L. Rev. 239, 245 (2009) (noting that "inside … corporate counsel" regularly conduct "internal compliance investigations"). And any fiduciary duty of corporate officers would likely be limited to the extent a court imposed a nondisclosure order on the relevant individual. *Cf. Fifth Third Bancorp v. Dudenhoeffer*, 573 U.S. 409, 428 (2014) (the "duty of prudence … does not require a fiduciary to break the law").

2. Ex Parte Filings: In attempting to meet its burden of justifying the nondisclosure order here, the Government has relied heavily on *ex parte* filings. *See* Microsoft Br. 12-14. The district court, in turn, denied Microsoft access to these filings—even though Microsoft is not the subject of the Government's investigation. *See id.* at 24, 41-42; JA-92 n.4. The strict-scrutiny analysis turns on fact-specific "proof" and "evidence" of narrow

tailoring. *Brown v. Entm't Merchs. Ass'n*, 564 U.S. 786, 800 (2011). Without access to the Government's factual assertions, Microsoft has been severely hobbled in trying to rebut the Government's narrow-tailoring arguments.

It is true that the Government may sometimes need to resort to *ex parte* filings, in order to conceal details of highly sensitive investigations. But in that scenario, courts must seek to reduce impairment of the adversarial process. *See Freedman v. Maryland*, 380 U.S. 51, 58 (1965) ("only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression"). In particular, courts should be especially vigilant to require "compelling … evidence" and "a direct causal link" between customer notification and harm to the investigation. *Brown*, 564 U.S. at 799-800. "[A]mbiguous proof" in the form of rote claims that notification *may* cause harm "will not suffice." *Id.* at 800; *see Doe*, 549 F.3d at 881, 885 (remanding where Government offered only the conclusory assertion that "disclosure … may endanger the national security of the United States"). And district courts should make detailed findings (even if maintained under seal) to facilitate effective appellate review. *Cf. United States v. Syks*, 637 F.3d 146, 152 (2d Cir. 2011) ("the district court must make findings with sufficient clarity to permit meaningful appellate review"). The

district court below did not follow these crucial steps. *See* Microsoft Br. 37-41.

In addition, to the maximum extent feasible, courts should require disclosure to the cloud service provider of the *general* nature of the Government's factual assertions. Such limited disclosures would give the cloud service provider an opportunity to identify less-restrictive alternatives and better equip it to evaluate the Government's narrow-tailoring arguments. These limited disclosures could be accomplished through filings under protective order or in redacted form. Here, the Government and district court failed to make even these minimal efforts to ensure a meaningful adversarial process. *See* Microsoft Br. 43; JA-92.

***3. Duration of Nondisclosure Order*:** A further defect in the nondisclosure order here is its prolonged duration. For 871 days and counting, Microsoft has been precluded from notifying its customer of the Government's SCA warrant and data seizure—and on July 31, 2020, the district court authorized extension of the nondisclosure order for yet another year. JA-108; *see id.* at 110 (rejecting Microsoft's motion to modify the extended order). As BSA has explained, "[t]echnology providers should not be restricted from notifying the subject of a data request unless non-disclosure is justified on an *exceptional basis* for a *limited duration*." BSA |

The Software Alliance, *Global Best Practices for Law Enforcement Access to Digital Evidence*, at 3 (emphasis added). The longer an investigation stretches on, the more time the Government has to make arrests, issue indictments, and obtain relevant information through other means. Naturally, then, its interest in suppressing a cloud service provider's speech should recede over time. It is already "rare that a regulation restricting speech because of its content will ever be permissible," *Playboy Entm't Grp.*, 529 U.S. at 818; to uphold such a restriction year after year should be extraordinary.

The constitutional difficulties with a prolonged nondisclosure order are compounded when the situation is viewed from the customer's perspective. Absent any notification from the Government or cloud service provider, the customer can be under investigation for years without ever knowing it. That result would hardly ever occur outside this unique SCA context. When the Government obtains a warrant to search a business's physical office, it generally arrives with the warrant, gives the business a copy, and leaves a receipt identifying any property seized. *See* Fed. R. Crim. P. 41(f)(1)(C). Even in the extraordinary circumstances in which the Government obtains a warrant to covertly search a person or business's physical property, it generally provides notice within thirty days. *See* 18

U.S.C. § 3103a(b)(3) (authorizing "sneak-and-peek" warrants).[20] While the Government may obtain extensions of that period "for good cause shown," *id.* § 3103a(c), those extensions rarely come close to the duration of the nondisclosure order here. In 2019, for instance, 83% of extensions were limited to ninety days.[21] The extended duration of the nondisclosure order here—which currently stands at 871 days—underscores the serious constitutional problems it poses.

CONCLUSION

Nondisclosure orders that violate the First Amendment erode the customer trust on which the cloud services industry depends. While law-enforcement needs may sometimes justify nondisclosure orders, the record here does not appear to meet the rigorous standards required to restrain a cloud service provider from speaking to its customer. The order thus violates the First Amendment. This Court should reverse the decision below and remand with instructions to modify the nondisclosure order in accordance with Microsoft's proposal.

---

[20] *See* U.S. Courts, *Delayed-Notice Search Warrant Report 2019* https://www.uscourts.gov/statistics-reports/delayed-notice-search-warrant-report-2019 (67% of delayed-notice warrants specified a 30-day delay).

[21] *See id.* (83% of extensions specified a 90-day period).

Respectfully Submitted,

Dated: December 21, 2020

By: /s/ Michael R. Dreeben

Yaira Dubin
O'Melveny & Myers LLP
7 Times Square
New York, NY 10036
(212) 326-2000
ydubin@omm.com

Michael R. Dreeben
Ephraim McDowell
O'Melveny & Myers LLP
1625 Eye Street, N.W.
Washington, DC 20006
(202) 383-5300
mdreeben@omm.com
emcdowell@omm.com

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Federal Rules of Appellate Procedure 29(a)(5) and 32(a)(7)(B) and Local Rules 29.1(c) and 32.1(a)(4)(A) because it contains 6,853 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in proportionally spaced typeface using Microsoft Word in 14-point Georgia font.

Dated: December 21, 2020

/s/ Michael R. Dreeben
Michael R. Dreeben

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of December 2020, I electronically filed the foregoing with the Clerk using the appellate CM/CF system. Counsel for all parties to the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: December 21, 2020

/s/ Michael R. Dreeben
Michael R. Dreeben